VŠB – Technická univerzita Ostrava

Fakulta elektrotechniky a informatiky

Katedra telekomunikační techniky

Problematika systémů detekce vniknutí IDS

Problematics of intrusion detection systems IDS

2009 Jakub Jaroš

Prohlašuji, že jsem tuto bakalářskou vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne 4. května 2009 ……

Rád bych poděkoval všem, kteří mi poskytli rady a připomínky při psaní této bakalářské práce, především pak vedoucímu mé bakalářské práce Ing. Pavlu Nevludovi.

Abstrakt

Práce pojednává o problematice systému detekce narušení a systému prevence proti narušení. Je zde vysvětlena funkce jednotlivých systémů a způsob jejich činnosti. Seznámení s IDS/IPS programem Snort. Popis režimů programu ve kterých pracuje, komponent, psaní pravidel a výstupu. Návrh testovacího laboratorního pracoviště a otestování jednotlivých systémů. Grafická prezentace problematiky pomocí Flashe.

Klíčová slova: systém detekce narušení, systém prevence proti narušení, Snort

Abstract

The work deals with the issue of intrusion detection system and intrusion prevention system. It is explained the various features and how do they work. Introduction to IDS/IPS via Snort program. Description of program modes in which it works, description of components, writing rules and output. Designing of the test laboratory workplace and testing of the individual systems. Graphical presentation about the problems using Flash technology.

Keywords: intrusion detection system, intrusion prevention system, Snort

Seznam použitých symbolů a zkratek:

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

VPN – Virtual Private Network

URL – Uniform Resource Locator

HIDS – Host-based Intrusion Detection System

NIDS –Network Intrusion Detection System

GUI – Graphical User Interface

HIPS – Host-based Intrusion Prevention System

NIPS – Network Intrusion Prevention System

DNS – Domain Name System

ICMP – Internet Control Message Protocol

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

MTU – Maximum Transmission Unit

Obsah

1. Úvod

V dnešní době velkého rozmachu internetu může útok na náš systém nebo síť přijít kdykoliv a odkudkoliv. Počítačová kriminalita patří k nejvíce se rozvíjejícím a nejvýnosnějším zločinům na světě. Počítačový útočníci se snaží využít neznalosti nezkušených uživatelů a hledají bezpečnostní mezery v aplikacích. Je tedy velmi důležité použití bezpečnostních systémů pro ochranu velmi citlivých dat. Mezi vhodné nástroje, jako součást zabezpečení, patří IDS a IPS systémy. Především pak volně dostupná aplikace Snort.

Bakalářská práce je členěna do pěti kapitol. Druhá kapitola popisuje systém detekce narušení (IDS) a systém prevence proti narušení (IPS). Je zde vysvětlena jejich funkčnost, kategorie systémů a způsoby detekce. Třetí kapitola se zabývá IDS/IPS programem Snort a jeho základním popisem. Ve čtvrté kapitole je popsána praktická část úlohy. Jsou zde uvedeny schémata laboratorního pracoviště, ukázky konfigurace a výstupy programu Snort.

Součásti bakalářské práce je CD nosič, na kterém jsou vytvořené Flash animace. Animace znázorňují návrh laboratorního pracoviště a vysvětlují funkce IDS a IPS systémů.

Předpokladem pro práci jsou základní znalosti o počítačových sítích a operačním systému Linux.

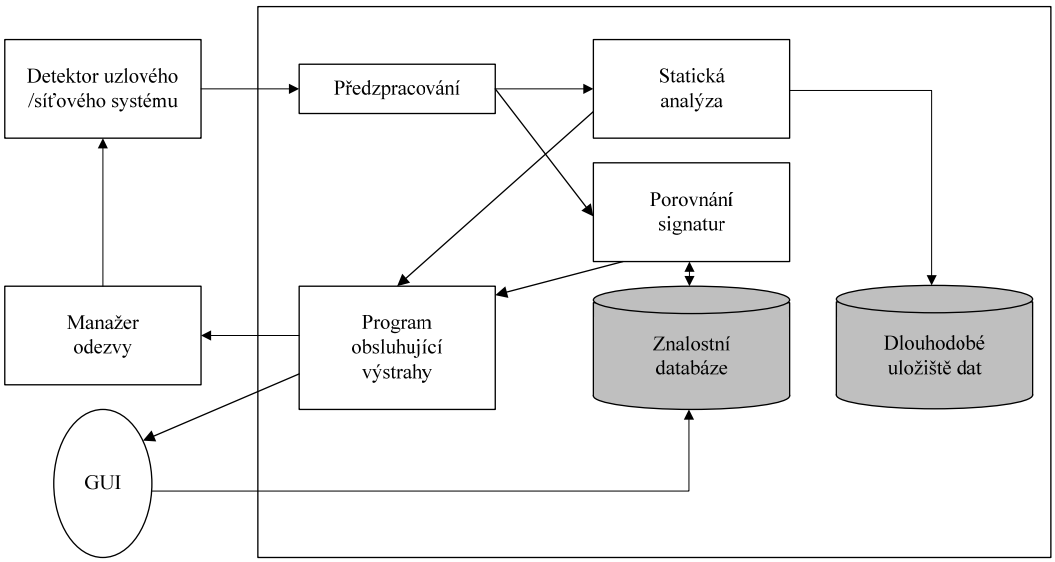
2. IDS a IPS

Systém detekce narušení (IDS) a systém prevence proti narušení (IPS) jsou nástroje zajišťující bezpečnost systémů a sítí. Jejich úkolem je hlásit nebezpečnou činnost a na základě těchto hlášení se ji snažit předejít. Nasazení systémů IDS a IPS nezaručí kompletní ochranu systému, jedná se jen o jednu část kompletního zabezpečení. Je tedy potřeba použít, dalších zabezpečovacích systému jako jsou firewall, antivir, VPN, URL filtr a další.

Narušením se rozumí například pokus o ovládnutí serveru, narušení integrity systému, zjištění přístupových hesel a získání citlivých dat.

2.1 IDS

IDS je systém detekující aktivity, které by se mohly jevit jako nebezpečné. Předpokládá se, že každá nebezpečná aktivita je odlišitelná od běžné aktivity uživatelů. Jedná se o pasivní systém, jehož úkolem není nebezpečným aktivitám zabránit, ale na tyto aktivity upozornit. Každopádně se jedná o důležitou součást zabezpečení, protože na základě těchto upozornění přijímáme příslušná opatření. Převzatý [1] obrázek 1 popisuje činnost IDS systému.



Obr. 1: Standardní IDS systém

2.1.1 Kategorie IDS systémů

IDS můžeme rozdělit do tří základních kategorií a to podle toho, jak jsou umístěné:

- Hostitelsky orientovaný IDS (HIDS)
- Síťově orientovaný IDS (NIDS)
- Hybridní

HIDS jsou systémy, které detekují nebezpečné aktivity přímo na daném hostiteli (Host-based IDS). Je tedy nutné nainstalovat daný software, přímo na každý hostitelský systém, kde ho chceme použít. Tyto systémy můžou pracovat samostatně, ale častěji jsou řízené z centrálního serveru. Tento způsob je nutný zejména u velkých sítí, kde je zapotřebí jednoduché řízení systémů, aktualizace databází signatur útoků a centralizované vyhodnocování. HIDS sledují procesy na daném hostiteli, vyhodnocují obsah logů a prověřují podezřelé chování uživatelů. Srovnávají jednotlivé události, zda se neshodují s databází signatur útoků.

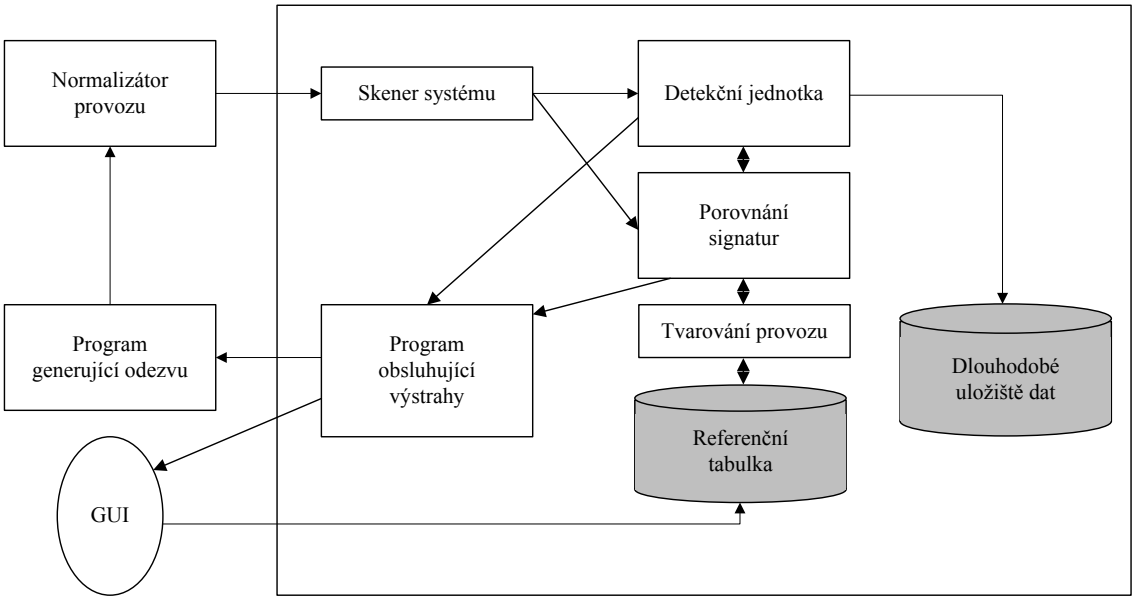
NIDS se umísťují do jednoho segmentu sítě (Network IDS) a kontrolují každý paket, který projde tímto segmentem. Tento systém tedy oproti HIDS hlídá větší skupinu zařízení. Jedná se o nejsnazší a nejrychlejší IDS systém, který ovšem trpí některými nedostatky. Hlavním problémem je velký objem zpracovaných dat. Hardwarové nároky se zvětšují přímo úměrně s počtem použitých pravidel, jelikož každý paket je nutné s těmito pravidly porovnat. Při použití velkého množství pravidel, pak může docházet k přetížení a mezitím může dojít k nepozorovanému útoku. Další velkou nevýhodou NIDS je vysoký počet falešných útoků. V tomto případě dochází k velmi obtížnému identifikování skutečného útoku. Je tedy nezbytně nutné mít systém profesionálně nastavený a tyto falešné útoky omezené na minimum. V opačné situaci může dojít k ignorování těchto hlášení a znehodnocení celého systému.

Hybridní IDS kombinuje oba předchozí systémy. Sleduje tedy jak síťový provoz, tak aktivity přímo na hostitelském systému.

2.2 IPS

IPS pracuje na podobném principu jako IDS, ze kterého se také vyvinulo. Rozdíl mezi nimi je v tom, že IPS se neumísťuje do sítě jako pasivní člen. IPS analyzuje všechny aktivity na

hostitelském systému nebo v síti. Když je vyhodnotí jako nebezpečné, tak je zablokuje. V tomhle se od IDS zásadně liší, protože na nebezpečné aktivity nereaguje pouhým varováním. Převzatý [1] obrázek 2 popisuje činnost IPS systému.



Obr. 2: Standardní IPS systém

2.2.1 Kategorie IPS systémů

Kategorie IPS systémů jsou podobné jako u IDS systémů. Jedná se opět o hostitelské IPS (HIPS), které fungují na hostitelském systému nebo o síťové IPS (NIPS), které sledují a blokují pakety procházející sítí.

2.3 Způsoby detekce IDS a IPS

Důležitou vlastností IDS a IPS systémů je způsob detekce narušení. Nebezpečné aktivity se zjišťují pomocí porovnávaní se vzory (pravidly), dlouhodobým sledováním normálního chování (zjišťování anomálií) a dalšími metodami. Nejpoužívanější bývají hybridní systémy, které

kombinují více způsobu detekce. Předpokladem správné detekce je, co nejmenší počet falešných hlášení vznikajících špatným vyhodnocením běžné činnosti.

2.3.1 Detekce porovnávání pomocí vzorů

Jedná se o jednu z prvních schémat pro detekování nebezpečných aktivit. Detekce porovnávání vzorů (pravidel, signatur) funguje na principu porovnávání událostí a posloupností událostí se vzory. Pomocí této metody se procházejí jednotlivé vzory v databázi a hledá se shoda s událostí. Dojde-li ke shodě, tak systém vygeneruje výstrahu. Pokud dojde jen k částečné shodě, tak systém prozkoumává další paket a zjišťuje, jestli nejde o posloupnost událostí, které jako celek mohou být nebezpečné. V případě nenalezené shody systém nijak nereaguje a událost bere jako běžnou činnost.

Velkou nevýhodou těchto systému je detekce jen předem definovaných událostí. Je tedy důležité tyto vzory neustále aktualizovat.

2.3.2 Detekce anomálií

Detekcí anomálií se rozumí odchylka od běžné aktivity. Jedná se o dlouhodobé sledování aktivit v průběhu určitého časového úseku (např. denní době), vytíženosti jednotlivých částí systému, chování uživatelů a dalších. Tyto systémy po zprovoznění sbírají informace o provozovaných aplikacích, protokolech a službách, zaznamenají si chování uživatelů a další aktivity. Takto si IDS/IPS vytvoří přehled aktivit v celém systému nebo síti a může přejít do plného provozu. Tento přehled aktivit se samozřejmě po určitém časovém úseku aktualizuje, aby byl stále přizpůsobený novým podmínkám (např. dlouhodobě zvýšený počet přístupů na server). Kompletní aktualizace může samozřejmě probíhat automaticky, a tím je celý systém jednodušší na údržbu.

Jako příklad použití detekce anomálií můžeme uvést sledování běhu DNS serveru. Pro tento příklad lze použít první dva zmíněné způsoby. Uvedeme si první, kterým je sledování DNS serveru v určitém časovém úseku (např. noční provoz). Dojde-li během této doby k zvýšenému počtu dotazů na DNS server, tak je tato činnost vyhodnocena jako nebezpečná.

Výhodou tohoto způsobu detekce je detekování i neznámých aktivit, které není potřeba přesně definovat. Hrozí zde, ale opět velké množství falešných útoků, protože nemůžeme předvídat chování uživatelů.

2.3.3 Ostatní způsoby detekce

Mezi další způsoby detekce můžeme zařadit systémy monitorování cílů, korelační a hybridní.

Systém monitorování cílu sleduje, zda dané cílové objekty byly změněny nebo modifikovány. Vše se provádí pomocí algoritmů vypočítávajících šifrovaný kontrolní součet daných objektů. V případě, že dojde ke změně objektu, tak systém na to upozorní.

Korelační systémy dlouhodobě sbírají data z více míst, které mohou mít nějakou vzájemnou souvislost.

Hybridní systémy kombinují více detekčních způsobů najednou, které nám jako celek zajistí dokonalejší detekci. Spojí se nám kladné funkce jednotlivých způsobů a záporné mohou být odstraněny právě jiným typem detekce.

2.4 Výhody a nevýhody IDS a IPS

Oba dva systémy mají své výhody i nevýhody. Nejideálnějším řešením je použití obou systému, protože se můžou vzájemně doplňovat.

Jako výhodu IDS systému můžeme uvést detekování vnějších i vnitřních útoků. Možnost centrálního řízení a vyhodnocování výstrah s více systémů pomocí jediné správcovské komponenty. Mezi nevýhody patří samozřejmě pasivnost celého systému. IDS útokům nijak nezabraňuje, ale jen generuje výstrahy. Další nevýhodou je už zmiňované velké množství falešných útoků. Tím se nám generuje opravdu velké množství varování. Tyto nasbírané data jsou pak náročné na diskový prostor, ale hlavně musí být následně všechny vyhodnoceny.

Hlavní výhodou IPS systému oproti IDS je, že se nejedná jen o pasivní systém. Nebezpečné aktivity jsou automaticky vyhodnocovány a provádějí se hned patřičné kroky (zabránění útoku). Toto řešení, ale může přinášet velké problémy. Celý systém potřebuje opravdu odbornou

konfiguraci a tím je celý systém velmi nákladný. V případě špatné konfigurace může totiž docházet ke špatnému vyhodnocování. Systém může pak vyhodnocovat některé normální aktivity jako nebezpečné a automaticky je blokovat, což přináší velké problémy.

3. Snort

Snort je program patřící do kategorie síťových IDS a IPS. Jde o open-source software a jedná se tedy o software s otevřeným zdrojovým kódem. Program lze volně šířit a je dostupný zdarma na stránkách autora [2]. V dnešní době se jedná o jeden z nejrozšířenějších IDS a IPS systému vůbec. Tento systém se neustále rozšiřuje a zdokonaluje. Díky jeho otevřenosti dochází k zdokonalování tohoto programu i díky jednotlivcům. Snort je IDS založené na pravidlech. Sleduje pakety procházející sítí a porovnává je se vzory. Dojde-li ke shodě, jsou prováděny předem definované kroky. Nejnovější verze obsahují i pokročilé způsoby detekce, jakou jsou detekce anomálií v síti.

3.1 Režimy Snortu

Snort pracuje ve čtyřech různých režimech:

- Sniffer mode (režim slídiče)
- Packet logger mode (režim záznamníku)
- NIDS mode (síťové IDS)

3.1.1 Sniffer mode

Tento režim zachytává data, která jsou obsažena v hlavičce a těle každého paketu. Tyto informace o každém paketu procházejícím sítí pak zobrazí na monitoru. Tento režim zobrazuje hlavičky paketů 2,3 a 4 vrstvy v OSI referenčním modelu a aplikační data.

Příkazy:

snort -d

Základní příkaz pro spuštění Sniffer mode.

snort – v

Zobrazení IP hlaviček (3. vrstva) a ICMP, TCP a UDP hlaviček (4. vrstva).

snort -ve

Zobrazení linkové vrstvy (2. vrstva), IP (3. vrstva) a ICMP, TCP a UDP hlaviček (4. vrstva).

snort -ved

Zobrazení předchozích vrstev a datových částí paketů.

3.1.2 Packet logger mode

Jedná se o rozšířený Sniffer mode, který zachycená data uloží do log souborů na pevný disk.

Příkazy:

snort -ved -l ./log

Využívá se předchozích příkazů pro sniffer mode (např. *snort -ved*), které jsou doplněny o příkaz specifikující cestu, kam se mají zachycená data ukládat.

snort -ved -l ./log –b

Při použití u vysokorychlostních sítí, kde je zaznamenáváno velké množství dat, se používá ukládání do binárních souborů (používá stejný formát ukládání dat jako program tcpdump).

snort -ved -r ./log/packet.log

Data uložená v binární podobě můžeme v programu Snort také otevírat pomocí změny příkazu (*-l* zápis, *-r* čtení).

snort -ved -r ./log/packet.log icmp

Pro lepší přehled nasbíraných dat můžeme použit filtry, pomocí kterých můžeme číst ze souboru jen potřebná data (např. ICMP filtr).

snort -ved -l ./log -h 10.0.0.0/24

Můžeme také nastavit rozsah IP adres sítě, ve kterých chceme zachytávat data.

3.1.3 NIDS mode

Jedná se o síťové IDS, které slouží ke sledování nebezpečných aktivit a upozorňuje na ně. NIDS mode se liší od předešlých tím, že nezaznamenává všechny aktivity v síti, ale jen ty potenciálně nebezpečné. Funguje na principu sledování paketů procházejících síti a porovnává je s předem definovanými pravidly. Teprve dojde-li ke shodě, tak se generuje výstraha. Tento způsob je tedy vhodnější pro následnou analýzu výstrah. Menší počet dat znamená menší požadavky na diskový prostor, ale především lehčí analýzu výstrah. Zde je nutné odborné nastavení systému, aby bylo co nejvíce omezeno generování falešných výstrah, které by celou následnou analýzu komplikovaly.

3.2 Komponenty Snortu

Snort je rozdělen do čtyř hlavních komponent:

- jednotka paketového záchytu
- zásuvné moduly preprocesoru
- detekční jednotka
- zásuvný modul pro výstup

Komponenty vzájemně spolupracují, zpracovávají data, vyhodnocují je a generují výstrahy.

3.2.1 Jednotka paketového záchytu

Úkolem této komponenty je sbírat data z pcap. Tyto data dále zpracovat a připravit pro detekční jednotku.

3.2.2 Zásuvné moduly preprocesoru

Komponenta prohlíží a testuje paketová data přijatá z pcap. Vyhledává také neobvyklosti v hlavičkách paketů. Jejím úkolem je předzpracování přijatých paketů pro detekční jednotku.

Rozhodne, co se má s každým paketem dělat – jestli se bude dále analyzovat, upravovat pro další zpracování, odmítne ho nebo vygeneruje výstrahu o nebezpečné činnosti tohoto paketu.

Tato komponenta se také stará o skládání souvisejících paketů. Objemnější data jsou totiž rozdělována do více paketů, jejichž velikost odpovídá MTU hodnotě. Jedná se o označení maximální velikosti IP paketu, který je možné přenést z jednoho síťového zařízení na druhé. Preprocesor tedy tyto pakety opět sjednotí a předá je k otestování. Tato činnost je velmi důležitá, protože i pokus o napadení může být rozdělen do více paketů. Pakety by pak mohly být samostatně vyhodnoceny jako neškodné. Musíme tedy kontrolovat kompletní celek, kde už lze odhalit nebezpečnou činnost.

3.2.3 Detekční jednotka

Jedná se o hlavní a nejdůležitější komponentu Snortu. Detekční jednotka se stará o testování jednotlivých paketů. Testování probíhá formou porovnávání paketů s pravidly. Každý paket je porovnán se všemi definovanými pravidly. Dojde-li ke shodě, tak je paket vyhodnocen jako nebezpečný.

Tato jednotka je velmi závislá na výkonu hardwaru, na kterém systém běží. Odvíjí se to od počtu pravidel, které jsou předem nadefinovány. S rostoucím počtem pravidel rostou i požadavky na hardware. V případě nedostatečného výkonu nebo velkého množství pravidel by totiž mohlo dojít k vynechávání jednotlivých paketů. U IDS systémů by tedy docházelo k nezkontrolování všech paketů a možnému nedetekování nebezpečné činnosti.

3.2.4 Zásuvné moduly pro výstupy

Úkolem této komponenty je generovat výstupní hlášení o každé zjištěné nebezpečné činnosti. Výstupní hlášení může být také zapisováno do binárních souborů v tcpdump tvaru, do MySQL databází, syslogů a dalších.

3.3 Pravidla Snortu

Program Snort obsahuje už v základu sadu pravidel, které můžeme využívat. Jeho největší výhodou je však možnost definování vlastních pravidel. Díky této možnosti si můžeme zabezpečení přizpůsobit požadavkům dané sítě. Takto nastavený systém bude pak sledovat jenom činnost, která je pro nás důležitá. Každé pravidlo se skládá z hlavičky a volby pravidla.

Obecný tvar pravidla

akce protokol zdr_IP zdr_port směr cíl_IP cíl_port (volby_pravidla)

3.3.1 Hlavička pravidla

Hlavička pravidla obsahuje akci, která se má vykonat, typ protokolu, zdrojovou IP adresu, zdrojový port, směr paketu, cílovou IP adresu a cílový port. Jednotlivé položky v hlavičce se oddělují mezerou a dají se vyjádřit také pomocí proměnných.

Proměnné

var HOME_NET 192.168.1.0/24

Vytvoří proměnnou HOME_NET, která bude představovat všechny IP adresy v rozmezí od 192.168.1.0 do 192.168.1.255.

Akce

action (aktivace) – vygeneruje výstrahu a testuje další dynamické pravidlo

dynamic (dynamika) – je nečinný do doby, než je vyvolán některým pravidlem z akce *aktivace*, teprve pak je tento paket zaznamenán

alert (výstraha) – vygeneruje výstrahu a daný paket zaznamená

pass (předání) – ignoruje definované pakety

log (zaznamenání) – zaznamená paket

drop (zahození) – zaznamená paket a přidá do iptables pravidlo o zahození paketu

reject (zamítnutí) – zaznamená paket a přidá do iptables pravidlo o zahození paketu, odešle TCP reset jedná-li se o TCP nebo ICMP protokol a zprávu o nedostupnosti v případě UDP protokolu

sdrop (zahození) – přidá do iptables pravidlo o zahození paketu, ale nezaznamená paket

Typy protokolů

Snort kontroluje *TCP*, *UDP* a *ICMP* protokoly. U každého pravidla si volíme, který protokol se bude kontrolovat.

Zdrojová a cílová IP adresa

Zdrojovou IP adresou definujeme adresu, odkud bude paket přicházet. Cílovou IP adresou zase, kam bude paket směřovat. Pomocí těchto nastavení můžeme definovat například rozlišování mezi vnější a vnitřní síti. IP adresy můžeme definovat několika způsoby:

192.168.1.1

Definování jediné IP adresy – adresa 192.168.1.1.

[192.168.1.1, 10.0.0.1]

Definování více IP adres – adresy 192.168.1.1 a 10.0.0.1.

192.168.1.0/24

Definování rozsahu adres – IP adresy v rozmezí od 192.168.1.0 po 192.168.1.255.

!192.168.1.1

Definování všech IP adres kromě zadané – všechny IP adresy kromě adresy 192.168.1.1.

any

Definování všech IP adres.

Zdrojový a cílový port

Zdrojovým portem se opět rozumí ten, z kterého je paket odeslán. Cílový port nám určuje port, na který paket směřuje. Porty můžeme definovat několika způsoby:

21

Definování jediného portu – port 21.

21:80

Definování rozsahu portů – všechny porty v rozmezí od 21 do 80.

:80

Definování rozsahu portů – všechny porty menší a rovny portu 80.

80:

Definování rozsahu portů – všechny porty větší a rovny portu 80.

any

Definování všech portů.

Směr paketu

Tento operátor nám určuje směr chodu paketu, který má být sledován. Tedy budou se sledovat jen pakety jdoucí daným směrem. Ukázka použití operandu:

log tcp 10.0.0.1 any -> 192.168.1.2 any

Zaznamená všechny TCP pakety jdoucí z adresy 10.0.0.1 na adresu 192.168.1.2. Pakety vysílané opačným směrem zaznamenány nejsou.

log tcp 10.0.0.1 any <> 192.168.1.2 any

Zaznamená všechny TCP pakety, které si zařízení s adresou 10.0.0.1 a 192.168.1.2 mezi sebou posílají.

3.3.2 Volba pravidla

Volba pravidla se definuje v kulatých závorkách za hlavičkou pravidla a jednotlivé pravidla se oddělují středníkem. Definují se zde výstrahy, které se budou generovat a další parametry paketu. Můžeme zde například určit, jak velké pakety se budou kontrolovat.

Můžeme zde definovat tyto pravidla, která lze rozdělit do tří skupin:

Obecná pravidla

Poskytují nám informace o pravidle, ale nemají žádný vliv na detekci.

msg: “Text”;

Text výstrahy, který se bude generovat k záznamu o paketu.

reference: <id system>,<id>;

Odkaz kde lze najít informace o této výstraze.

gid: <generator id>;

Informuje, která část Snortu vyvolala výstrahu.

sid: <snort rules id>;

Jednoznačná identifikace pravidla.

rev: <revision integer>;

Jednoznačná identifikace přepracovaných Snort pravidel.

classtype: <class name>;

Kategorizace pravidla.

priority: <priority integer>;

Definování priority útoku.

metadata: key1 value1;

Dodatečné informace o pravidle.

logto:"filename";

Zaznamenání výstrahy do daného souboru.

Pravidla testující data paketu

content: "<content string>";

Prohledá paket, jestli neobsahuje definovaný řetězec.

nocase;

Nebudou se rozlišovat velká a malá písmena. Používá se především s pravidlem *content*.

offset: <number>;

Tato hodnota nám určí, o kolik bajtů se posune počáteční pozice pro hledání řetězce.

dsize: >number;

Porovnávání velikosti paketu. Definujeme si například, jaká velikost paketu je nebezpečná. Udává se v bajtech.

Pravidla testující hlavičku paketu

ttl: <value;

Porovnává hodnotu životnosti paketu.

flow: [(established|stateless)]

[,(to_client|to_server|from_client|from_server)]

[,(no_stream|only_stream)];

Definování pravidla jen pro některé činnosti.

3.5 Výstup Snortu

Po definování pravidel Snortu a spuštění systému je velmi důležité pochopit výstupní hlášení. Teprve až po správné analýze výstupu můžeme podniknout potřebná opatření.

Ukázkový výpis

[**] [1:384:5] ICMP PING [**]

[Classification: Misc activity] [Priority: 3]

04/17-10:23:11.435987 10.0.0.2 -> 192.168.1.2

ICMP TTL:63 TOS:0x0 ID:0 IpLen:20 DgmLen:1028 DF

Type:8 Code:0 ID:26901   Seq:3 ECHO

Popis jednotlivých položek výpisu

[1:384:5]

První číslo nám udává, která část Snortu výstrahu vygenerovala. Druhé číslo jednoznačně identifikuje pravidlo. Třetí číslo jednoznačná identifikace přepracovaného Snort pravidla.

ICMP PING

Označení výstrahy, které se zadává pro jednoduchou identifikaci.

[Classification: Misc activity]

Zařazení výstrahy do skupiny – skupina Misc activity.

[Priority: 3]

Závažnost výstrahy – závažnost 3.

04/17-10:23:11.435987

Čas kdy byla výstraha zaznamenána.

10.0.0.2

IP adresa zařízení, ze kterého paket pocházel.

192.168.1.2

IP adresa zařízení, kam paket směřoval.

ICMP

Typ protokolu.

TTL:63

Životnost paketu (počet směrovačů, kterými může projít – max. 255).

TOS:0x0

Typ služby.

ID:0

Identifikace paketu.

IpLen:20

Velikost IP hlavičky.

DgmLen:1028

Velikost celého paketu.

DF

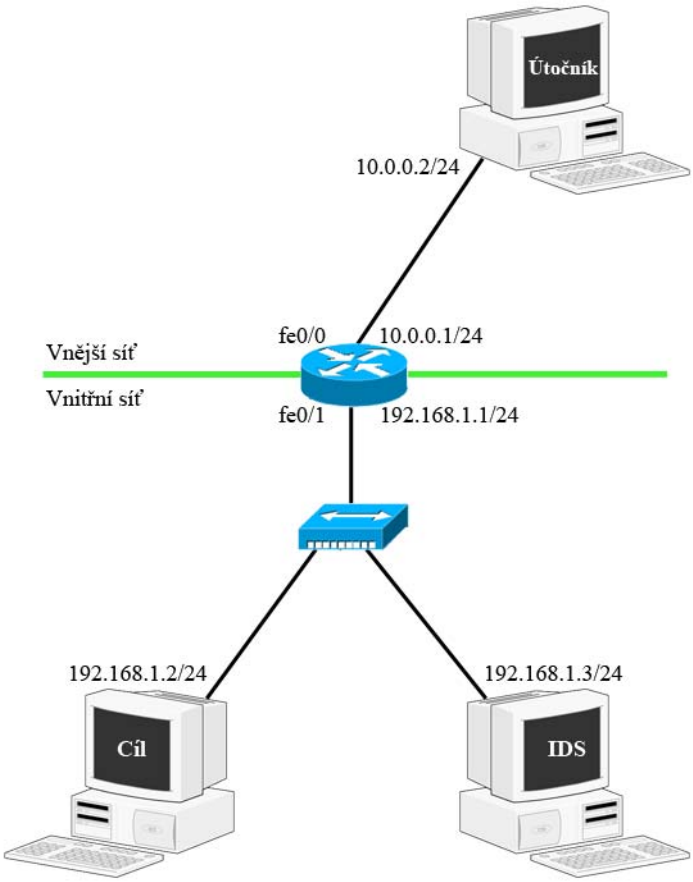
Fragmentace – DF(Don´t Fragment – Nefragmentovat).

4. Praktická část

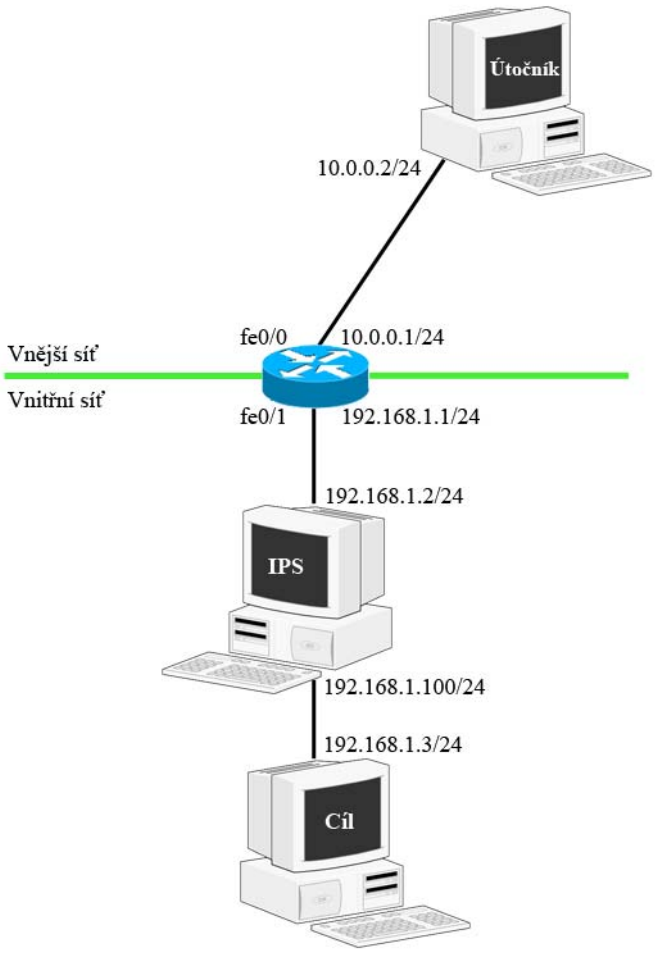
Praktická část byla provedena v laboratoři N312. Ta je vybavena všemi potřebnými zařízeními, která jsou vhodná k vytvoření zkušebního pracoviště.

4.1 Návrh pracoviště

Pracoviště bylo navrženo s ohledem na to, aby co nejlépe simulovalo skutečný provoz. Na obrázcích 3 a 4 jsou znázorněna schémata pracovišť. Pomocí směrovače jsem vytvořil dvě sítě – vnější a vnitřní síť. Vnitřní síť nám simuluje například podnikovou síť (zde může běžet HTTP a FTP server nebo zde může být podniková databáze). Vnější síť můžeme brát například jako internet.



Obr. 3: Schéma zapojení pro testování IDS



Obr. 4: Schéma zapojení pro testování IPS

Moje laboratorní pracoviště se skládá ze tří počítačů s operačním systémem Linux, jednoho směrovače a rozbočovače. Ve vnitřní síti jsou umístěné dva počítače. Jeden počítač je brán jako cíl a na druhém je nainstalován IDS/IPS program Snort. Počítač ve vnější síti představuje útočníka a budou z něho probíhat útoky. V praxi samozřejmě nebude cílem jen jediný počítač, ale může jít o celou podnikovou síť. Pro otestování však stačí jen jediný cíl, protože Snort hlídá celou vnitřní síť. Takže systém funguje stejně při sledování sítě o jednom počítači jako u sítě obsahující stovky počítačů.

4.2 Konfigurace zařízení

Útočník

ifconfig eth0 10.0.0.2 netmask 255.255.255.0

route add default gw 10.0.0.1

Cíl

ifconfig eth0 192.168.1.2 netmask 255.255.255.0

route add default gw 192.168.1.1

IDS

ifconfig eth0 192.168.1.3 netmask 255.255.255.0

route add default gw 192.168.1.1

Na tomto počítači byl nainstalován IDS/IPS program Snort. Byla zde použitá linuxová distribuce Debian, protože tato distribuce obsahuje balíček Snort, je tato instalace velmi jednoduchá. Pro nainstalování stačí příkaz:

apt-get install snort

IPS

Použito předchozí nastavení jako u IDS, jen byla navíc nakonfigurovaná druhá síťová karta.

ifconfig eth1 192.168.1.100 netmask 255.255.255.0

Konfigurace směrovače

V zapojení jsem použil směrovač od firmy Cisco Systems. Směrovač se pro konfiguraci propojuje s počítačem přes konzolový port. Jeho konfigurace probíhá pomocí programu Minicom.

Nastavení směrovače pro moje zapojení:

enable

configure terminal

interface FastEthernet0/0

ip adress 10.0.0.1 255.255.255.0

no shutdown

exit

interface FastEthernet0/1

ip adress 192.168.1.1 255.255.255.0

no shutdown

4.3 Ukázka výstrah Snortu

Pro lepší přehled ukážu pár výstrah z jednotlivých režimů Snortu.

4.3.1 Sniffer mode

Spuštění příkazem:

snort –v

Pro otestování jsem zadal na počítači útočníka příkaz ping, směřující na cíl:

ping 192.168.1.2

Snort vygeneroval výstrahu:

04/17-10:43:15.691638 10.0.0.2 -> 192.168.1.2

ICMP TTL:63 TOS:0x0 ID:0 IpLen:20 DgmLen:84 DF

Type:8 Code:0 ID:59412   Seq:2 ECHO

4.3.2 Packet logger mode

Spuštění příkazem:

snort –ve –l /etc/snort/log

Pro otestování jsem zadal na počítači útočníka příkaz ping, směřující na cíl:

ping 192.168.1.2

Snort vygeneroval výstrahu:

04/17-10:44:46.380737 0:1E:F7:AC:4A:63 -> 0:30:5:8E:5E:19 type:0x800 len:0x62

10.0.0.2 -> 192.168.1.2 ICMP TTL:63 TOS:0x0 ID:0 IpLen:20 DgmLen:84 DF

Type:8 Code:0 ID:3349   Seq:2 ECHO

4.3.3 NIDS mode

Jelikož je tento režim založený na pravidlech, tak jsem si pro ukázku vytvořil konfigurační soubor – snort.conf:

###

var HOME_NET 192.168.1.0/24

#Definování proměnné HOME_NET pro celou vnitřní síť.

var EXTERNAL_NET !192.168.1.0/24

#Definování proměnné EXTERNAL_NET pro všechny IP adresy mimo vnitřní síť.

var RULE_PATH /etc/snort/rules

#Definování proměnné RULE_PATH jako cestu složky obsahující pravidla, která jsou už

#součástí programu.

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING";

classtype: misc-activity; priority: 3; dsize: >150; sid: 384; rev: 5;)

#Vygeneruje se výstraha s názvem ICMP PING v případě, že je na počítač ve vnitřní

#síti vyslán ICMP paket z počítače mimo vnitřní síť, který je vetší než 150 bajtů.

include $RULE_PATH/ftp.rules

#pomocí příkazu include můžeme použít pravidla, která jsou v programu integrované

output log_tcpdump: tcpdump.log

#Zápis výstrahy v binárním tvaru ve formátu tcpdump.

###

Pro otestování jsem zadal na počítači útočníka příkaz ping o velikosti 1000 bajtů, směřující na cíl:

ping 192.168.1.2 –s 1000

Snort vygeneroval výstrahu:

[**] [1:384:5] ICMP PING [**]

[Classification: Misc activity] [Priority: 3]

04/17-10:23:11.435987 10.0.0.2 -> 192.168.1.2

ICMP TTL:63 TOS:0x0 ID:0 IpLen:20 DgmLen:1028 DF

Type:8 Code:0 ID:26901   Seq:3 ECHO

5. Závěr

Díky této bakalářské práci jsem pochopil princip funkce systému detekce narušení (IDS) a systému prevence proti narušení (IPS). Naučil jsem se pracovat s programem Snort, který funguje na principu těchto systémů.

Při návrhu laboratorního pracoviště jsem využil získaných znalostí z předmětu Počítačové sítě. Na tomto pracovišti jsem testoval funkce programu Snort a snažil se detekovat a blokovat nebezpečné aktivity. Na základě návrhu laboratorního pracoviště a testování těchto systémů jsem vytvořil Flash animace popisující jejich činnost.

IDS a IPS se neustále rozvíjí a vylepšují. V dnešní době především systém prevence proti narušení, který je jako aktivní ochrana používanější. Snahou vývojářů je vytváření nových schémat detekce, která budou pracovat inteligentněji a samostatněji. Systémy by pak měli i bez předem definovaných vzorů odhalit nebezpečnou činnost. Především kvůli velké vynalézavosti útočníků jde o velmi důležitý krok.

Literatura

[1] ENDORF, Carl, SCHULTZ, Eugene, MELLANDER, Jim. *Hacking : detekce a prevence počítačového útoku*. 1. vyd. Praha : Grada Publishing, 2005. 356 s. ISBN 80-247-1035-8.

[2] ROESCH, Martin. *Snort : the de facto standard for intrusion detection/prevention* [online]. 2009 [cit. 2009-04-18]. Dostupný z WWW: <www.snort.org>.

Přílohy

[1] Flash animace na přiloženém CD nosiči.